AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method for performing cryptographic operations using keys obtained from ~~generating~~ random numbers that are generated using the Data Encryption Standard (DES) algorithm with a secret key K, said method taking as input a random integer s of size 64 bits, and an integer m, said method sending back as output m 64-bit random integers x_1, x_2, ..., x_m, said method comprising the following ~~three~~ steps:

1) With the DES algorithm and using the key K, encrypt a value D representing date data and put the result in an integer variable I;

2) For j in the range 1 to m:

2a) Replace s by s XOR I,

2b) ~~Put in the~~ Define an integer variable y equal to the result of the encryption of s with the DES algorithm using the key K,

2c) Put in xj the result of y XOR s,

2d) Replace s with y XOR I,

2e) Put in s the result of the encryption of s with the DES algorithm using the secret key K; ~~and~~

3) Return as output the succession (x_1, x_2, ..., x_m); and

4) Performing cryptographic operations with keys corresponding to said values x_1, x_2, ...x_m.

2. (Currently Amended) A method for ~~generating~~ performing cryptographic operations using keys obtained from random numbers, said method taking as input a random integer s of size 64 bits and an integer m, and sending back as output m 64-bit random integers x_1, x_2, ..., x_m, by using the Data Encryption Standard (DES) with a secret key K, an integer intermediate variable y, and a source S ~~of quality deemed to be insufficient~~ of random integers on 64 bits x_1, x_2, ..., x_m, said method comprising the following ~~two~~ steps:

1) For j in the range 1 to m:

1a) Generate an integer I by means of the source S,

1b) Replace s with s XOR I,

1c) Put in y the result of the encryption of s with the DES algorithm using the key K,

1d) Put in x_j ~~xi~~ the result of y XOR s,

1e) Replace s with y XOR I,

1f) Put in s the result of the encryption of s with the DES algorithm using the key K; ~~and~~

2) Return as output the succession (x_1, x_2, ..., x_m); and

3) Performing cryptographic operations with keys corresponding to said values x_1, x_2, ..., x_m.

3. (Currently Amended) A handheld, wearable, or portable electronic device that executes the following steps to generate m 64-bit random integers x_1, x_2, ..., x_m:

1) With the DES algorithm and using a key K, encrypt a value D representing date data and put the result in an integer variable I;

2) For j in the range 1 to m:

2a) Replace a random integer s by s XOR I,

2b) Put in an integer variable y the result of the encryption of s with the DES algorithm using the key K,

2c) Put in x_j the result of y XOR s,

2d) Replace s with y XOR I,

2e) Put in s the result of the encryption of s with the DES algorithm using the secret key K; and

3) Return as output the succession (x_1, x_2, ..., ~~xm~~ x_m).

4. (Previous Presented) An electronic device according to claim 3, wherein said device is a smart card.

5. (Previous Presented) An electronic device according to claim 3, wherein said device is a contactless card.

6. (Previous Presented) An electronic device according to claim 3, wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

7. (Previous Presented) An electronic device according to claim 3, wherein said device is a badge.

8. (Previous Presented) An electronic device according to claim 3, wherein said device is a smart watch.

9. (Currently Amended) A handheld, wearable, or portable electronic device that executes the following steps to generate m 64-bit random integers x_1, x_2, ..., x_m:

1) For j in the range 1 to m:

1a) Generate a 64-bit random integer I,

1b) Replace a 64-bit random integer s with s XOR I,

1c) Put in an integer variable y the result of the encryption of s with the DES algorithm using the key Y,

1d) Put in ~~xi~~ x_j the result of y XOR s,

1e) Replace s with y XOR I,

1f) Put in s the result of the encryption of s with the DES algorithm using the key K; and

2) Return as output the succession (x_1, x_2, ..., x_m).

10. (Previous Presented) An electronic device according to claim 9, wherein said device is a smart card.

11. (Previous Presented) An electronic device according to claim 9, wherein said device is a contactless card.

12. (Previous Presented) An electronic device according to claim 9, wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

13. (Previous Presented) An electronic device according to claim 9, wherein said device is a badge.

14. (Previous Presented) An electronic device according to claim 9, wherein said device is a smart watch.